学校编码：　　分类号_____密级_____

学号：X2012230179　　UDC _____

厦门大学

工 程 硕 士 学 位 论 文

某市电子政务安全管理体系分析与实施

Analysis and Implementation of the E-Government Security Management System for a City

指导教师姓名：　董槐林 教授

专　业 名 称：　软件工程

论文提交日期：　2014 年 05 月

论文答辩时间：　2014 年 05 月

学位授予日期：　　年　月

指　导　教　师：_____

答辩委员会主席：_____

2014 年 05 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下,独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　√　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

随着我国城市化步伐的加快，城市化的发展进入一个的高速时期。电子政务作为数字化城市建设的重要内容，将会成为整个城市的信息枢纽。目前，电子政务网络开始进入到宽带化、层次化、分组化的发展阶段，越来越多的政府部门开始使用电子政务来进行日常的办公、OA 管理、统计以及日常的决策等业务，政府部门的办公也开始实现了网路化和数字化，因为政府部门的办公内容中涉及到很多的国家机密信息，因此，需要加强电子政务的安全管理，这对于促进我国的电子政务快速的发展以及构建信息化的社会都具有很重要的意义。

本文针对贵州的一个地级市作为研究对象，首先对国内外的电子政务的安全管理的相关研究内容进行了细致的分析，结合地级市的特点，对该市电子政务的现状以及存在的问题进行详细的分析，指出该市目前电子政务在安全管理上的缺陷。然后，结合这些提出的问题，设计了该市的电子政务安全控制系统的框架结构模型，从安全技术、安全组织管理、法律法规、安全风险等多方面对安全体系模型进行分析和论述。寻求了几种可用的电子政务安全建设方案，从而保证了该市的电子政务能够安全稳定的运行。

关键词：电子政务；安全管理体系；数字城市

Abstract

With the acceleration of urbanization and the rapid development of information technology in recent years, our city has entered a rapid development stage. E-government is a strategic leader of digital city construction, is the nerve center of the digital city. With hierarchical grouping of government as well as the development of broadband networks, government decision-making more and more business statistics, daily supervision and inspection services, OA, such as the management of operations and comprehensive business-oriented multimedia are beginning to digital, network transition, there is a lot of important information related to the relevant state and government, therefore, to strengthen research on e-government security issues, to promote the healthy development of China's e-government, and society as a whole process of information has important significance.

According to a Guizhou city as the research object, first security management of E-government in China and the related research contents in detail,combined with the characteristics of the prefecture level city, a detailed analysis on the current situation of e-government and the existing problems,points out the defects of current e-government in the safety management ofthe city. Then, according to these problems, designs the framework model of E-government security control system of the city, from the security technology,security organization and management, laws and regulations, safety risks and other aspects of the analysis and discussion of the security system model. Forthe few available e-government security construction scheme, so as to ensure the E-government the city can be safe and stable operation.

Key Words: E-Government; Security Management; Digital City

目 录

CONTENTS

第一章 绪论

1.1 选题背景及意义

电子政务是指政府部门和机构通过使用计算机网络的相关技术，开展日常的办公活动，通过电子政务的改造能够使得政府的工作更加标准化、信息化、公开化以及服务化，我国的信息改革工作正不断的在推进，电子政务在我国政府中得到了快速的发展和应用，政府工作出现了网上办公、一站式电子政务服务、门户网站等新型办公方式，这些新方法大大的提高了政府的服务能力和办事效率，给政府的工作带来较大的便利，但是由于接入了网络给政府内部的信息安全构成了威胁。

电子政务是目前新兴的一种政府办公方式，电子政务是一种采用现代化的计算机以及信息技术来提高政府部门和机关的办事效率以及服务能力，通过电子政务能够实现网上办公和服务，超越了空间和时间的限制，使得整政府的工作更加的高效、廉洁、简便。政府部门的作用是实现政府的职能，是关系到国家政务的，涉及到的工作内容是保密性的，但是电子政务是一个有互联网、内网（办公业务层和核心数据层）以及外网所构成的信息系统，这样一个如此复杂的应用环境将会给整个系统带来一些安全上的隐患，因此需要对安全问题进行强化，其信息的安全问题体现在：

1、电子政务是一种政务活动的新表现，具有安全性需求和开放性需求，这两者是一个矛盾。政府部门需要提供一些公众所需要的信息，就需要通过网络的方式与外界网络实现连接，这样才能将政府内部的一些有用信息共享给公众并提供相应服务，但接入网路后也会给这些信息的安全带来危害，防止一些不法分子对这些数据进行盗取和攻击。需要妥当的处理安全和开放之间的关系。

2、信息技术的快速发展也带来了黑客攻击手段的不断提升，攻击的手段和方法越来越先进和高明，不能简单的通过安装杀毒软件就能保证信息的安全，虽然杀毒软件时不断进行升级的，但是保护的能力依然有限。为了解决这些问题，必须从技术和管理两个层面出发，结合技术和管理，为电子政务的安全目标提供一个有力的保障。

3、因为政府部门中的很多信息和数据都是属于机密性的，为了保证这些信息和数据的安全，些黑客的入侵、病毒的破坏和信息的泄露都会造成巨大的损失和社会危害。为了保证电子政务系统的安全运行，需要建立一个长期的规划，技术和管理上都要实现动态化，需要建立一个健全的动态化保障体系。

我国的政府机构中，地级市的电子政务系统建设是非常重要的，是整个国家信息化建设的关键所在。因此，本课题针对贵州省的一个地级市的电子政务系统进行研究，从安全管理体系建立出发，对安全管理过程中所存在的问题和系统所需要解决的问题进行研究，对与我国的其他同一级别的地级市的电子政务的安全保障体系的建设将具有重要的参考和借鉴意义。

1.2 电子政务的安全管理问题

政府的信息化是政府部门的一种改革，会涉及到很多关于政府核心的信息，有的信息还可能是涉及到国家机密的信息，因此电子政务的首要任务就是安全，电子政务的安全性直接关系到国家的安全，保证电子政务的安全就是保证国家的利益。是保证社会稳定的前提，电子政务能够大幅度的提高国家政府部门的办公效率和服务职能，人们的生活以及企业的经营都非常依赖电子政务，一旦出现安全问题，会给社会到来较大麻烦

电子政务系统的安全保证不完全是依靠技术来好实现的，还需要加强安全的管理。安全技术是一种控制安全的手段，为了保证安全技术的效果，还需要通过一些管理措施来保证其实施，不然，安全技术最终会失败和僵化。管理就是指信息安全管理，是对安全技术的催化，只要全面的至始至终实施安全管理，才能保证信息的长期稳定性的安全。大多数的安全隐患和安全时间，主要的原因就是由于管理上的缺陷而造成的，因此需要在意识上重视安全管理对于保障信息安全的重要性。我们经常提到的信息安全就是三分技术七分管理，最重要的在于对信息的安全管理。

总的来说，电子政务的安全实际就是信息的安全管理，信息安全管理就是采用一些安全手段来保证信息的可用性、机密性、完整性的方式来实现信息资产的保护，是一种指导和规范信息安全的活动和过程。信息安全管理是整个信息安全

保障体系中的核心部分，信息安全的管理对指导信息安全体系的建设、保护信息的资产以及降低风险上都具有非常重要的作用，信息安全管理涉及很多的知识，如控制目标的选择、评估风险、规范化流程制作、安全信息政策的制定以及相关人员的安全意识培训。

1.3 国内外研究综述

目前，国内外主要从两个方面对电子政务的安全进行研究，也就是风险管理和信息安全管理模型，下面我们针对这两个领域进行国内外研究现状的介绍。

1、信息安全管理模型研究

目前国内外较为成熟的安全管理模型有：国际网络安全协会所提出的一种信息安全管理生命周期法的模型-ISML[2]，这一模型是在 BS7799 基础上发展起来的，因此经常称之为 PDCA 模型[3]；美国的 entasafe vigilEnt 公司的安全专家 harles Cresson Wood 提出了一个关于信息安全策略的生命周期模型；印度的 James B.D.Joshi 在 web 的基础上提出了信息安全系统的安全管理模型。除此之外，S.A.Kokolakis 还在对业务过程建模的基础上对信息系统的安全进行了分析和设计，提出了一种新型的观点就是将组织业务过程和安全风险相结合分析；K.Juszczyszyn 也提出了一种多级安全模型，该模型是通过着色 Petri-net 语义来进行描述的，模型主要用于对企业的网络进行安全分级；B.Moore 和 E.Ellesson 等人总结了大量的研究结果在此基础上给出了安全策略的框架模型，并指出 7 条安全的策略规则。

我国在信息安全管理方面的研究也取得了一些成果，如专家陈伟、孙强等人所提出的 HTP 模型[4]；徐春根通过大量的研究提出了动态的模型，通过使用角色登台的概念采用 RP 来指代角色被激活，在此基础上通过 RP 语境来动态的控制权限，实现了动态的控制 访问权限[5]；曹阳等人提出了一种基于三视图框架的分布式信息系统安全体系结构，其中的三视图分别是安全技术、安全组织管理和安全服务，在此基础上对信息系统的安全进行了描述[6]；段海新等人通过大量的研究计算机网络的安全性，最后提出了一种保证计算机网络安全的体系机构，在该结构中用视图的方式将网络安全体系分成了安全服务、安全的实体以及安全周期这几个内容，并对三者这件的关系和相关规则进行了描述[7]；我国的一些软

件研究室同样开展了这方面的研究如中软信息安全实验室。研究者申雅琴结合该研究院的一些研究成果，提出了一种可适应性的网络安全管理模型，称之为P2DR[8]。

2、风险管理研究

信息安全管理体系的核心内容就是对风险的控制和管理，安全管理规则和措施的制定的目的就是为了实现最大化降低风险，提高系统稳定性，从而保证系统能够长期稳定的运行。风险评估的好坏关键在于对评估标准的好坏，是风险评估有效性的主要依据，目前主要的标准有 C、BS7799、SSE-CMM 等。

风险评估是信息安全管理系统中的一个重要内容，是设计一个有效的信息安全管理系统的前提条件。目前国内外已经有大量有效的安全评估模型，比如OCTIVE、APPDRR、 NISTSP800-30、ISO13335 等，这些都是非常经典的风险评估模型。此外，有学者提出一个机构在面临安全问题以及解决安全问题会花费大量成本时，需要对整个信息系统可能存在的风险和后果进行全面的分析之后，才能从本质上去描述安全问题，并制定一个非常有效的安全问题解决方案[9]。Bilar D.提到软件本身的缺陷和脆弱性会导致风险的存在，风险高于阀值之后，需要更换相关软件来实降低风险[10]。这种方法虽然能够进行成本的控制，但是实际的应用中所取得的效果还需要进一步的研究。西班牙政府针对自己的国情提出了 MAGERIT 风险分析以及管理方法的模型[11]。美国审计总局相关人员通过对风险管理周期、风险评价表、风险管理程序以及风险评估矩阵的有效利用取得了较好的风险控制效果[12]。

我国目前正在不断的加快信息安全的一些标准的建设，国家也发布了相关的准则。国内的很多学者也进行了较多的研究，如广东电信科学技术研究院的研究人员卫成业通过大量的研究后，在可能性以及后果的基础上提出了的风险评估模型[13]；黄勤、张月琴等人也提出了一种信息安全评估模型，通过系统的聚类法来建立的风险模块化的评估模型[14]；范雯等人经过研究提出了一种基于决策的风险管理模型，并给出了安全策略的效益的算法[15]；杜人杰结合了层次分析法和故障树分析法，在此基础上建立了电子政务的信息安全三元集成法，这一方法是对可操作的关键威胁以及资产的薄弱环节评估的一种改进和创新[16]；汤志伟，高天鹏等人阅读了大量文献和通过实践经验提出了一种基于模糊算法的电子政务信息

风险评估方法，这一方法是理论的依据是资产的弱点评估以及可操作的关键威胁（Operationally Critical Treat，Asset，and Vulnerability Evaluation）这两个方法[17]；李慧，刘东苏等人通过评估结果和风险分析的方式形成安全需求，在此基础上进行安全措施的制定[18]。随着信息安全问题的日益增加，风险评估的相关研究得到了不断的重视和加强，风险的评估以及相关的模型也不断的在升级和创新，这些都为信息安全控制提供了更多的理论支持。

3、电子政务安全管理相关研究

电子政务的安全管理的研究我们从国家的宏观层面、企业和组织层面以及学者专家等微观层面这三个部分分别进行阐述。

(1)国家宏观层面

主要是电子政务的安全立法和安全组织：

a . 国家在安全立法方面，国外的发达国家已经颁布了大量的电子政务的相关法规和指南，美国在 2000 年就颁布了《政府信息安全改革法案》；日本在 2000 年也颁布了相关法规来保证政府的电子政府信息的安全；英国在 2000 年颁布了《政府现代化白皮书》。我国的相关法律颁布相对晚一些，在 2005 年 9 月颁布的《电子政务信息安全等级保护实施指南》，同时一些其他的法规、法律、地方政府以及标准中都涉及到电子政务安全管理方面的内容，但是总体上没有形成体系的法规，还需要进一步的完善。

b．安全组织的管理上，各个国家的政府建立来相关的组织机构来进行电子政务的实施的管理，比如美国国家的信息技术理事会、爱尔兰国家也成立了相应的小组进行政府信息化管理，我们国家虽然也成立了一个专门的小组进行国家信息化的管理和领导，但是针对电子政务方面的管理没有相应的机构来管理，原因是因为电子政务是一个复杂度较高且范围较广的系统。

(2)企业和组织的中观层面

企业方面主要是中观层面上进行信息安全管理，如一些企业、高校或者地方的政府所提出的一些解决方法，如美国的 IBM 公司就提出了一种 Tivoli 电子政务的安全整合平台[19]、我国的明朝万达公司推出的 Chinasec 电子政务进行等级保护的解决方案[21]、赛迪顾问集团提出的的电子政务安全系统(V2.O)[20] 、吉林大学的吉大正元提出的基于 PKI/PMI 的电子政务系统应用的安全解决方案[23] 、

天华公司提出的解决方案[22] 。很多的地方政府也提出了一些与自身特点相符的电子政务信息的安全解决方案和项目，湖南省政府经济研究信息中心就针对湖南省的电子政务进行了一个网络安全问题的设计和解决[24]、浙江省台州市的信息中心针对该市的特点寻求了一种解决对策[25]，宜昌市政府在“全网部署、一体安全、简单为本”这一原则的基础下建立了宜昌市的电子政务网络的安全屏障，我国的国信办在 2005 年到 2006 年期间在天津、河南、重庆以及广东进行了电子政务安全工作的试点，工作取得了非常大的成效，但是需要对着西成功经验进行进一步总结和推广。

(3)专家及学者的微观层面

电子政务在整个国家都具有非常重要的地位，很多的学者和专家对此开展了大量的研究，也取得了较多的成果，从国外的研究来看，2001 年的美国学者 LM.Zeichner 就通过研究向美国国家的电子政务的一些安全性提出了建议[26]，建议由：颁布相关的面向风险管理的政策，对 IT 行业以及服务提供商进行安全的规范；政府部门需要对 IT 的安全以及提供相应的安全服务；政府要对安全管理的方法进行深入研究，建立正确的风险分析和相应的模型。2002 年 N.Boudriga 学者对整个电子政务系统所存在的安全风险以及挑战进行详细的分析，指出了在电子政务中采用入侵检测、访问授权以及身份认证这些内容的重要性，强调了安全的重要性[27]。2003 年的 S.Cohen 对电子政务的问题和未来的发展方向进行了阐述，提出电子政务发展中的一个最大问题就是要解决安全的问题，指出需要将非技术的问题同技术问题相结合，包括一些相应法律的建立等[28]。2004 年的 F.Arcieri 等人对一种安全基础的结构方案进行了定义并得到了实现，这一方案被用于居民的个人数据系统中[30]；除此之外，还有大量的的学者提出恶劣相应的电子政务安全模型和措施，如 S.Benabdallah、Kaliontzoglou 等分别提出了具体的实施模型和基于 WEB 的电子政务平台等[31] [32] 。

我国的电子政务安全方面的研究较国外而言，起步较晚，但是也取得了一定的成果，比如，杜虹等人通过对电子政务的研究，将其划分成公共服务、非涉密和涉密三个等级，对不同安全等级的网络的隔离盒信息交换技术进行了介绍[33]。赵宏志、蔡瑜坤等人通过研究和分析了国内外在计算机立法上的区别，提出我国需要针对电子政务方面加强法规以及 CA 认证体制的建设[34]；加强对电子文档、

数字签名和政府信息公开和保密等方面的立法。我国的沈昌祥院士通过研究提出的一种具有“三层次两中心”结构的电子政务信息安全的保障体系[35]、周杨、王春枝等人提出并构建了一个基于 PKI 的电子政务的安全体系的策略[38]、石继华等人针对基于面向服务类的软件架构提出了电子政务安全保护的方法[37]、蒋兴浩对电子政务的安全结构进行了六个层次的划分[39]、胡心雷、胡晓勤等人在互联网的基础山提出了电子政务信息安全的相关对策等[40]。

总的来说，我国目前在学术界关于电子政务的安全管理的研究还处于起步阶段，安全管理体系建设问题上还处于发展的初期，相关的理论知识的研究较少，大多的文献和期刊主要是对国外知识的总结和综述。目前，整个学术界都普遍的认可了电子政务安全管理需要将技术和非技术相结合这一观点，但是系统且完整的安全管理理论还没有形成。因此我国在进行电子政务安全管理方面的研究上可以对国外的先进经验和技术进行借鉴。

1.4 本文的研究内容与结构

图 1-1 给出了本论文的整体研究技术路线。

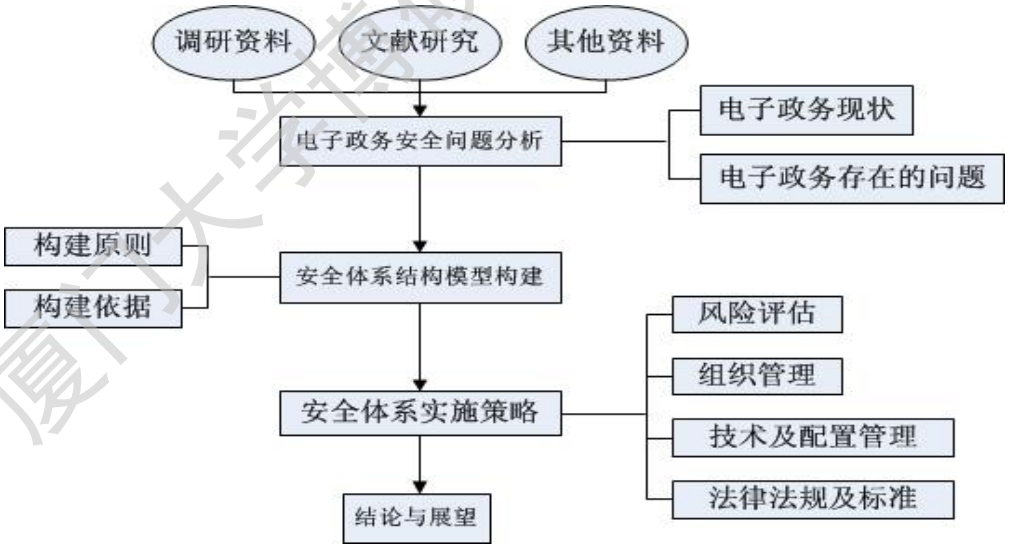

图 1-1 论文研究技术路线图

本文首先分析了国内外电子政务安全管理的研究现状，在此基础上对地级市的电子政务信息安全的特点进行总结，分析了目前存在的问题和威胁所在，指出了贵州的一个地级市在电子政务安全管理上的问题。针对这些问题，提出和设计